UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

RAYNIER RAMIREZ, ***individually and on behalf of all others similarly situated,***

Plaintiff,

v. **Case No.____**

DOLLAR TREE, INC. and

ZEROED-IN TECHNOLOGIES, LLC,

Defendants,

CLASS ACTION COMPLAINT

COMES NOW Plaintiff Raynier Ramirez, individually and on behalf of all similarly situated persons, by counsel, and for his Complaint against Dollar Tree, Inc. ("Dollar Tree") and Zeroed-In Technologies, LLC ("Zeroed-In") (collectively, "Defendants"), he states as follows:

INTRODUCTION

1. Dollar Tree, Inc. is a leading operator of discount variety stores operating under the brands Dollar Tree and Family Dollar, and is headquartered in Chesapeake, Virginia. It has over 200,000 employees.

2. Amongst other systems, Dollar Tree uses human resources (HR) software provided by Zerod-In.

3. Zeroed-In is a company that operates in the realm of workforce analytics, offering a specialized software solution that incorporates artificial intelligence (AI) to enhance the capabilities of human resources (HR) departments. Its software automates the data science

elements within HR, providing a means for organizations to utilize their HR data for economic gain.

4. In August of this year, Zeroed-In learned that Dollar Tree's use of its Zerod-In system had been infiltrated by unauthorized individuals ("The Breach"). The Breach led to the compromise of files, which included sensitive information pertaining to employees and clients of Dollar Tree.

5. Zeroed-In notified Dollar Tree of the breach on August 31st. Dollar Tree failed to notify its current, former, and prospective employees affected by the incident until almost 3 months later.

6. On November 27, 2023, Zeroed-In reported a data security incident with the Office of the Maine Attorney General and, on the same day, began sending out data breach letters to individuals whose information was compromised because of the data security incident ("Notice Letter").

7. In the filing with the Office of the Maine Attorney General, Zeroed-In revealed Personally Identifiable Information (PII) of numerous individuals is believed to have been exposed by the Data Breach.[1] The Office of the Maine Attorney General report noted that the data breach was not discovered until August 31, 2023.

8. The Notice Letter issued fails to specify the exact date on which The Breach was detected, only noting that the review of the incident was concluded on August 31, 2023.[2] Zeroed-In has stated that certain customers were informed during the investigation process. However, a significant number of individuals were not notified until much later, approximately four months

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/b3993ddd-2443-4645-ae45-f36dc7686236.shtml (last visited Dec. 13, 2023).
[2] *Id.*

afterward, on November 27, 2023, in receipt of the Notice Letter. In these delayed notifications, Zeroed-In indicated that the compromised information included names, dates of birth, and/or Social Security numbers present in their systems at the time of The Breach.

9. Dollar Tree mandated that its employees, including the Plaintiffs and Class Members, provide sensitive and non-public PII as a prerequisite for their employment. This requirement was a standard condition of their employment agreements or contracts.

10. The Defendants have retained this sensitive PII for extended periods, often spanning several years. This retention has frequently continued even after the end of the business relationship between the consumer (employee) and the Defendants, leading to prolonged exposure of the data.

11. By acquiring, processing, utilizing, and financially benefiting from the Plaintiffs' and Class Members' PII, the Defendants effectively undertook legal and ethical responsibilities. These responsibilities included the duty to safeguard the PII from unauthorized access, breaches, and other forms of data intrusion, upholding a standard of care commensurate with the sensitivity of the information.

12. However, the Defendants failed to implement adequate security measures to protect this PII. Essential security practices, such as data encryption and redaction, were not sufficiently employed, leaving this highly sensitive information vulnerable to potential breaches and unauthorized access.

13. Consequently, the Defendants' negligent or careless approach, combined with their significant failure to implement robust protective measures for sensitive employee data, led to serious data security lapses. This negligence resulted in the PII being stored in an unencrypted and unprotected state, significantly increasing the risk of data breaches and unauthorized access.

14. The impact of such negligence is far-reaching, as it not only compromises the immediate security of the PII but also exposes the individuals to potential long-term risks such as identity theft, financial fraud, and other personal and professional repercussions. The Defendants' failure to adhere to standard data protection practices reflects a disregard for the privacy and security of the individuals whose data they were entrusted with.

15. Plaintiffs and Class Members brings this lawsuit representing all individuals whose PII was compromised due to Defendants' shortcomings in several critical areas: (i) ensuring adequate protection of the PII of Plaintiffs and Class Members; (ii) informing Plaintiffs and Class Members about Defendants' deficient information security practices; and (iii) securing hardware that stored protected PII through reasonable and effective security measures free of vulnerabilities and incidents. The actions, or lack thereof, by Defendants constitute, at a minimum, negligence and represent a breach of various federal and state laws.

16. Defendants neglected the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to establish and uphold adequate and reasonable security measures, and by not ensuring adherence to these measures by their IT vendors. This failure extended to protecting the PII of Plaintiffs and Class Members, neglecting to take available actions to prevent unauthorized data disclosure, and failing to adhere to applicable, mandatory, and appropriate standards, protocols, and procedures for data encryption, even for internal purposes.

17. Consequently, the PII of Plaintiffs and Class Members was compromised, leading to its disclosure to unknown and unauthorized third parties.

18. Following the compromise and subsequent unauthorized disclosure of the Plaintiffs and Class Members' PII, it likely fell into the hands of various unknown third parties with diverse

motives. These parties could range from cybercriminals and hackers, who might exploit the stolen PII for identity theft, financial fraud, or selling it on dark web marketplaces, to data brokers interested in aggregating this personal information for resale to advertisers and marketers.

19. Additionally, competing corporations or businesses may acquire this PII illicitly for competitive advantages or corporate espionage. Scammers could utilize this information for phishing attacks and fraud, while marketing firms might target the affected individuals with unsolicited advertising. Moreover, ransomware attackers could leverage the PII for extorting money.

20. The unauthorized disclosure of PII thus poses numerous risks, including privacy invasion, financial and identity theft crimes, and unwanted solicitations, with the challenge that once PII is compromised, its containment and protection from further misuse become increasingly difficult.

21. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

22. Plaintiffs and Class Members have suffered injury due to Defendants' actions. The injuries they have suffered include, but are not limited to: (i) invasion of privacy; (ii) depreciation in the value of their PII; (iii) time and opportunity costs expended in efforts to mitigate the fallout from the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in unsolicited spam calls, texts, and emails; and (vi) ongoing and heightened vulnerability of their PII, which: (a) remains unencrypted and susceptible to unauthorized access and exploitation; and (b) continues to be stored by Defendants, thus facing ongoing risks of unauthorized disclosure unless Defendants implement adequate protective measures.

23. The Plaintiffs and Class Members initiate this legal action on the grounds of Negligence, Negligence Per Se, Breach of Implied Contract, and, alternatively to Breach of Implied Contract, Unjust Enrichment. This lawsuit seeks to address and rectify the damages incurred due to the Data Breach and to implement measures preventing future breaches. It represents not only the Plaintiffs and Class Members but also all others in similar situations whose personal information was compromised and stolen as a result of the Data Breach. The ongoing risks associated with the Defendants' inadequate data security practices are a central concern of this action, highlighting the need for comprehensive remedial measures to enhance data protection and prevent future breaches. The legal action underscores the sustained vulnerability of the affected individuals and aims to hold the Defendants accountable for their failure to uphold the necessary standards of data security and protection.

PARTIES

24. Plaintiff Raynier Ramirez is, and at all times mentioned herein was a resident of the State of Florida.

25. Plaintiffs and Class Members are current and former employees at Zeroed-In's clients, including Dollar Tree that were exposed to The Breach.

26. Defendant Zeroed-In is a foreign limited liability corporation.

27. Defendant Dollar Tree is a corporation incorporated in Virigina, with its principal place of business at 500 Volvo Parkway, Chesapeake, Virginia 23320.

JURISDICTION AND VENUE

28. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

interest and costs. The number of class members is in the millions, many of whom reside outside the Commonwealth of Virginia. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

29. This Court has general personal jurisdiction over Dollar Tree because it is headquartered in this District. This Court has specific personal jurisdiction over Zeroed-In in this case because Zeroed-In purposely availed itself by transacting with Dollar Tree with respect to Plaintiffs' claims.

30. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to this action occurred in this District, Defendants have harmed Class Members residing in this District, and Defendants are subject to the Court's personal jurisdiction with respect to this action. Further, the primary torts and injuries originated and occurred here.

FACTUAL ALLEGATIONS

A. Background

31. Zeroed-In is a provider of HR analytics software.[3] The company boasts over 30,000 registered users and claims to manage data related to 2.7 million work lives within its databases.[4]

32. Dollar Tree is a client of Zeroed-In and operates a network of over 8,000 low-priced retail stores across the United States and Canada. Dollar Tree forms a significant part of Zeroed-In's clientele.

33. Plaintiffs and the Class Members consist of current, former, and prospective employees of Dollar Tree.

34. As a prerequisite for employment, clients of Zeroed-In, such as Dollar Tree, mandate that their employees, which include the Plaintiffs and Class Members, submit highly

[3] **https://www.zeroedin.com/about-zeroedin/ (last visited Dec. 13, 2023).**
[4] ***Id.***

sensitive PII. Zeroed-In, in turn, derives economic benefits from handling this PII, signifying its value to the company's operations.

35. At the time of the Data Breach, the Defendants were in possession of unencrypted personal information belonging to the Plaintiffs and Class Members. This information, crucial and confidential in nature, was stored without adequate encryption, underscoring the vulnerability and potential risk of exposure faced by the affected individuals.

36. Upon information and belief, Dollar Tree assured its employees, including the Plaintiffs and Class Members, about the safety and confidentiality of the PII collected from them as a requirement for employment. These assurances included commitments to maintaining the privacy of such information and to delete any sensitive data once its retention was no longer necessary.

37. In providing their PII to the Defendants, the Plaintiffs and Class Members did so with the reasonable expectation and mutual understanding that the Defendants would fulfill their obligations to ensure the confidentiality and security of this information, safeguarding it against unauthorized access.

38. The Plaintiffs and Class Members have consistently taken appropriate measures to keep their PII confidential. They relied on the Defendants' technical expertise and assurances to maintain the security and confidentiality of their PII, using it solely for authorized disclosures. The importance that the Plaintiffs and Class Members place on the confidentiality of their PII is paramount, and they have an expectation for reasonable security measures to protect their sensitive information.

39. Defendants have a legal duty to keep consumer’s PII safe and confidential. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class

Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of their IT vendors and affiliates.

40. Defendants had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

41. Zeroed-In's Privacy Policy provides that: "[w]e employ robust security measures to protect against the loss, misuse and alternation of the personal information under our control. The Sites employ Secure Socket Layer (SSL) technology using both server authentication and data encryption. The Sites are hosted in a secure server environment that uses firewalls, intrusion detection systems, and other advanced technology to protect against interference or access from outside intruders."[5]

42. Similarly, Dollar Tree's Privacy Policy provides that: "[w]e use various reasonable and appropriate safeguards (administrative, organizational, technical, electronic, procedural, and physical) to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of confidentiality, integrity, and availability of your Personal Information."[6]

43. The Defendants derived financial gains from the collection and use of the Plaintiffs and Class Members' personal information, which was a crucial aspect of their business operations. However, in this process, the Plaintiffs and Class Members did not receive the expected benefits from this exchange and were, instead, adversely affected.

44. The concept of "benefit of the bargain" implies that in a contractual agreement, all parties should receive the anticipated benefits as per the terms of the contract. In this scenario,

---

[5] https://www.zeroedin.com/privacy-policy/ (Last visited December 13, 2023).
[6] https://www.dollartree.com/privacy-policy (Last visited December 13, 2023).

while the Defendants capitalized on the personal information for their financial and operational advantage, the Plaintiffs and Class Members did not receive the corresponding benefit, which would include the assurance of data security and privacy.

45. Instead, they found themselves in a detrimental position, with their sensitive information compromised and exposed to risks they had not agreed to undertake. This failure to provide adequate data security measures, despite the implied promise to do so, signifies a breach of the implicit contract, leaving the Plaintiffs and Class Members vulnerable and without the full protection and security they were led to expect.

B. The Data Breach

46. According to the Notice Letter, Zeroed-In first discovered suspicious activity in its systems on August 8, 2023, and completed its investigation and "a review of the contents of the systems to what information was present at the time of the incident and to whom the information relations" on August 31, 2023.[7] Nevertheless, it took an additional 3 months, until November 27, 2023, to notify Plaintiffs and Class Members of the Data Breach.[8]

47. Under § 18.2-186.6 of the Virginia Code, entities must promptly notify affected individuals and the Office of the Attorney General of any breach of unencrypted personal information that risks identity theft or fraud. This notification must detail the incident, the compromised data types, protective actions taken, and provide advice for vigilance. The notification is required "without unreasonable delay" post-discovery. Additionally, if over 1,000 individuals are notified, consumer reporting agencies must also be informed.

48. Though there can be exceptions if additional time is needed to ascertain the full extent of The Breach or if law enforcement indicates that an immediate notification might

[7] **Ex. A.**
[8] ***Id.***

compromise an ongoing investigation. However, based on the Notice Letter, Zeroed-In reported that the investigation was concluded on August 31, 2023. Indicating there was no need for unnecessary delay.

49. Defendants offered no explanation for the delay between the initial discovery of The Breach and the belated notification to affected individuals– delay that resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

50. The Notice Letter failed to provide comprehensive information regarding the Data Breach's root cause, the specific vulnerabilities exploited, and the exact remedial measures implemented to prevent future breaches.

51. To this day, these essential details remain undisclosed to Plaintiffs and Class Members, who have a significant interest in ensuring the continued protection of their PII.

52. The lack of such critical information impedes their ability to fully understand The Breach's implications and to take appropriate measures to safeguard themselves against potential future risks stemming from this incident.

53. Defendants neglected to implement security procedures and practices commensurate with the sensitivity of the information held for the Plaintiffs and Class Members. This negligence led to the exposure of their PII. Furthermore, Defendants demonstrated a lack of due diligence in the selection of their vendors and in their decisions about sharing sensitive PII.

54. The Breach resulted in unauthorized access and acquisition of unencrypted PII belonging to the Plaintiffs and Class Members, including names, birth dates, and Social Security numbers. This personal information was compromised and extracted during The Breach.

C. Defendants Knew of the Risk

55. The obligations of the Defendants to ensure data security were of heightened significance in light of the marked increase in cyber-attacks and data breaches aimed at institutions responsible for collecting and storing PII, such as the Defendants, prior to the occurrence of this particular breach.

56. Defendants, being custodians of highly sensitive PII, it was well within the knowledge and understanding of the Defendants that unprotected PII is not only valuable but also a prime target for criminal entities. These entities often seek to exploit such information through unauthorized access.

57. In light of recent high profile data breaches at other industry leading companies, Defendants, as a custodian of PII, knew or should have known that the data they collected and maintained would be targeted by cybercriminals.

58. The Defendants were, or reasonably should have been, aware of the critical importance of securing the PII entrusted to them by the Plaintiffs and Class members. Given the prevalent risks in today's digital landscape, the Defendants had a duty to anticipate and guard against the potential consequences of a breach in their data security systems, or those employed by their vendors. Such consequences, which were both foreseeable and preventable, include the substantial and significant costs that have been, and continue to be, borne by the Plaintiffs and Class Members as a direct result of the Defendants' failure to adequately protect their sensitive data.

59. Despite awareness and the foreseeable risks associated with data security negligence, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

60. At all relevant times, the Defendants were, or should have been, fully cognizant of the critical necessity to protect the PII of the Plaintiffs and Class Members. This understanding extended not only to the importance of safeguarding this data but also to fully grasping the significant and foreseeable consequences of any breach in their data security system.

61. Defendants knew or should have known, that a breach would not only compromise the integrity of the data but also impose substantial costs and damages upon the Plaintiffs and Class Members.

62. Defendants were, or should have been, aware of both the unique nature and the considerable volume of the PII stored on their servers. This data encompassed thousands of individuals, thereby amplifying the severity and scope of harm that would be inflicted upon these individuals in the event of the data being exposed, particularly if left unencrypted.

63. The offer contained in the Notice Letter to provide 12 months of credit monitoring falls significantly short of a proper remedy. This service primarily serves to alert individuals to potential misuses of their personal information, but only after such misuse has already occurred. Given the nature of data breaches and the subsequent misuse of stolen information, the actual impact of the Data Breach may not manifest until several years later. Therefore, a mere 12-month coverage of credit monitoring does not align with the potentially prolonged window during which the stolen data could be misused, leaving individuals vulnerable and unprotected long after the expiration of the monitoring service.

64. Furthermore, Zeroed-In's proposition to provide credit and identity monitoring implicitly acknowledges the compromise of the Plaintiffs and Class Members' sensitive PII within the Defendants' computer systems. This offer serves as an admission that the PII was not only accessed and affected but was also compromised and extracted from their systems. The harm

suffered by the Plaintiffs and Class Members can be traced directly and proximately back to the Defendants' inability to implement or maintain sufficient data security measures, revealing a clear causation.

65. Stolen PII, especially critical data like Social Security numbers, can lead to prolonged and repeated misuse, resulting in sustained harm to the victims over several years.

66. As a corporation that held the PII of employees and former employees, the Defendants had a responsibility to understand the significance of protecting this data and to foresee the potential consequences of a breach in their security systems.

67. These consequences extend to substantial costs incurred by the Plaintiffs and Class Members due to The Breach. Despite this knowledge, the Defendants did not adopt adequate cybersecurity measures to avert the data breach, thereby neglecting their duty to safeguard the sensitive information entrusted to them.

D. Defendants Failed to Comply with Industry Standards and Federal and State Law

68. The Defendants not only retained and stored the Plaintiffs' and Class Members' PII, but they also derived significant financial benefits from it. The Defendants' ability to perform their services hinges on the possession of Plaintiffs' PII.

69. By obtaining, collecting, using, and deriving a financial benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

70. The Defendants were bound by industry standards as well as federal and state laws to ensure the confidentiality of Class members' Private Information and protect it against unauthorized access and disclosure.

71. When Plaintiffs and Class members entrusted their Private Information to the Defendants, they did so with the reasonable expectation and mutual understanding that the Defendants would fulfill their duty to keep this information confidential and secure it from unauthorized access.

72. The Defendants' negligence in providing adequate security measures to safeguard the Private Information of Plaintiffs and Class members is particularly alarming given the nature of their industry. Human resources platforms, such as those operated by the Defendants, have been increasingly targeted by bad actors seeking to illicitly access customers' Private Information. These platforms are deemed highly susceptible to data breaches by cybersecurity experts due to the value of the sensitive information they handle.

73. The Plaintiffs and Class Members have consistently taken reasonable measures to ensure the confidentiality of their PII. They trusted the Defendants to maintain the confidentiality and security of their PII, use it solely for business purposes, and only allow authorized disclosures.

74. The Defendants had the capability to avert this Data Breach by effectively securing and encrypting the files and servers that stored the PII of the Plaintiffs and Class Members. This could have been achieved through diligent selection and thorough auditing of their IT vendors' security measures and software.

75. At the very least, Defendants were obligated to adopt industry-recommended best practices to ensure robust data security. This includes mandating the creation of strong passwords by users, a fundamental step in protecting accounts from unauthorized access. Using Two-Factor Authentication to prevent unauthorized access or Encrypting data into a format unreadable without a specific decryption key, thereby securing the information even in the event of unauthorized

access. Additionally, the implementation of multi-layer security measures, such as firewalls and anti-malware software, is essential to defend against various cyber threats.

76. Furthermore, it is imperative to regularly update and patch all systems with the latest security software. This practice is vital to protect against newly emerging vulnerabilities and cyber threats. Alongside these technical measures, there is a significant need for improved employee education regarding safe data security practices. Training employees to recognize and respond appropriately to potential security threats is a critical component of a comprehensive data security strategy. By failing to implement these essential practices, the Defendants neglected their responsibility to safeguard the sensitive data entrusted to them, exposing the data to avoidable risks, and failing to adhere to industry standards.

77. The Defendants were on notice that under the Federal Trade Commission (FTC) Act, they are barred from participating in "unfair or deceptive acts or practices in or affecting commerce." The FTC has determined that a company's neglect in upholding reasonable and appropriate data security measures for individuals' sensitive personal information constitutes an "unfair practice," which is in direct contravention of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

78. In October 2016, the Federal Trade Commission (FTC) refined its cybersecurity recommendations for businesses in its publication "Protecting Personal Information: A Guide for Business." These guidelines emphasize the importance for businesses to safeguard employee personal information. Key measures include proper deletion of unneeded personal data, encryption of information on computer networks, understanding network vulnerabilities, and implementing corrective policies for security issues. Businesses are advised to use intrusion detection systems for early breach detection, monitor incoming traffic for both anomalous and signature-based

threats, be vigilant for large data transfers indicating potential breaches, and have a breach response plan in place.

79. Furthermore, the FTC advises companies to only retain PII as long as necessary for transaction authorization, restrict access to sensitive data, enforce complex network passwords, employ industry-tested security methods, monitor networks for unusual activities, and ensure that third-party service providers also have reasonable security measures in place.

80. The retention of sensitive data by Defendants, beyond the necessary scope of their business operations or legal requirements, suggests that the companies held onto this information primarily for its own benefit. Zeroed-In potentially leveraged the data for purposes such as analytics, marketing, or other business-related activities that serve the company's interests.

81. The Defendants neglected to adhere to these essential security precautions, as evidenced by the fact that cybercriminals were able to access individuals' Private Information from Defendants systems and network.

82. The Breach indicates a lapse in the implementation of effective security measures that could have prevented or minimized the extent of unauthorized access to sensitive data.

83. Defendants were at all times fully aware of this obligation to protect the PII on their networks yet failed to comply with such obligations.

E. Defendants Breached Their Common Law duty of Care in Inadequately Safeguarding Plaintiffs' and Class Members' Data.

84. Alongside their legal responsibilities under federal and state laws, the Defendants had a duty of care towards the Plaintiffs and Class Members. This duty involved exercising reasonable care in acquiring, retaining, securing, and safeguarding the PII in their possession. It required them to protect this information from being compromised, lost, stolen, accessed, or

misused by unauthorized persons. Furthermore, the Defendants were obligated to provide a level of security consistent with industry standards and to ensure that their computer systems, networks, and protocols were robust enough to protect the PII of Plaintiffs and Class Members adequately.

85. The Defendants demonstrated a clear breach of their duty of care through negligence and recklessness in several critical aspects of data security management. Their failure to adequately maintain and secure their computer systems and data, coupled with insufficient auditing and monitoring of their data security practices, led to significant vulnerabilities. The specific areas of failure include, but are not limited to:

a. The absence of a robust data security system, which is essential for minimizing the risk of data breaches and cyberattacks. This includes the lack of advanced security technologies and protocols that could have deterred or detected unauthorized access.

b. Ineffective protection of employees' PII, indicating a lack of proper security measures like encryption, access controls, and secure data storage practices.

c. A failure to actively monitor their data security systems, which is critical for early detection and response to potential breaches or suspicious activities within their network.

d. Negligence in auditing or overseeing the data security practices of their vendors, thereby extending the risk of breaches through third-party associations.

e. Inadequate training provided to employees and vendors in the proper handling and protection of PII, leading to mishandling or exposure of sensitive data.

f. Non-compliance with Federal Trade Commission (FTC) cybersecurity guidelines, which set standards for data protection and privacy, thus violating provisions of the Federal Trade Commission Act (FTCA).

g. Disregarding established industry standards for cybersecurity, which include best practices and protocols that are widely recognized and adopted for data security.

h. Additional breaches of their obligations to safeguard the PII of the Plaintiffs and Class Members, which could encompass a range of lapses in security practices and data management protocols. Systems, which contained unsecured and unencrypted PII, due to their negligent and unlawful failure to safeguard this sensitive information.

86. If the Defendants had remedied the vulnerabilities in their information storage and security systems—including those of their vendors and affiliates—followed industry guidelines, and implemented expert-recommended security measures, they could have prevented the unauthorized access and theft of the Plaintiffs' and Class Members' confidential PII. The Defendants' lack of action in this regard constitutes a clear failure to uphold their duty to safeguard the sensitive information entrusted to them.

F. Exposure to Risk

87. The Plaintiffs and Class members have suffered harm due to the exposure of their Private Information in the Data Breach. This breach has led to significant risks of identity theft, financial loss, and other related harms.

88. The theft of the Plaintiffs' and Class members' Private Information indicates a high probability that this information is now available for purchase by cybercriminals. Such availability increases the likelihood of further misuse of this information in the future.

89. The unencrypted PII of Class Members is likely to be trafficked on the dark web, a common practice among hackers. Moreover, this PII might also be acquired by companies for unauthorized targeted marketing, making it easily accessible to unauthorized entities.

90. The connection between data breaches and the risk of identity theft is straightforward and well-documented. Criminals often steal PII to monetize it, typically by selling it on the black market. This stolen data is then used by other criminals to commit various identity theft-related offenses.

91. Private Information is highly coveted by identity thieves, as acknowledged by the FTC. This information can be exploited to commit various crimes, including identity theft and financial fraud.[9] There exists a well-established "cyber black market" where stolen Private Information is traded on underground internet platforms, often referred to as the dark web.

92. The monetary value of the compromised Private Information is significant. Research has shown that the average direct financial loss per victim of identity theft was approximately $1,349 in 2014.[10]

93. The FTC has recognized personal data as a valuable commodity. As highlighted by former FTC Commissioner Pamela Jones Harbour, the vast collection and commercial value of such data are often not fully understood by the general public. Data is considered a form of currency, with larger datasets offering more potential for analysis and profit.[11]

94. Reflecting the high value placed on personal information, some companies now provide individuals with opportunities to monetarily benefit from their Private Information. This

---

[9] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[10] *See* U.S. Dep't of Justice, Victims of Identity Theft, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf

[11] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

model aims to empower individuals with more control over their information and its distribution, while also allowing them to profit from these transactions. This approach has fostered a new marketplace for buying and selling valuable personal data.[12]

95. Considering the Defendants are in the business of selling personal data, the Defendants were, or should have been, fully aware of the high sensitivity of the Private Information they held and its potential misuse by third parties for wrongful acts like identity theft and fraud.

96. If the Defendants had addressed their security system flaws, adhered to industry standards, and implemented expert-recommended security measures, they could have averted The Breach and the subsequent theft of Plaintiffs' and Class members' Private Information.

97. The Private Information compromised in the Data Breach is extremely valuable to hackers and thieves and can be used in various malicious ways. Information about an individual can be combined with other data, enhancing its value and utility for criminal activities.

98. Moreover, with technological advancements, computer programs with AI and extensive internet scanning capabilities can assemble a mosaic of information. This 'mosaic effect' can link disparate pieces of data to individuals in ways previously unfeasible, exacerbating the risks associated with The Breach.[13]

99. These extensive dossiers can then be continuously sold and resold to dishonest entities and criminals, such as illegal telemarketers, perpetuating the cycle of misuse and exploitation of the victims' personal information.

---

[12] *Web's Hot New Commodity, supra* note 17.

[13] The mosaic effect: the revelation risks of combining humanitarian and social protection data (February 9, 2021) https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/

100. The Private Information compromised in the Data Breach is of substantial value to hackers and cybercriminals. The data is vulnerable to a range of illegal uses, including the establishment of new credit and financial accounts under the victims' names.

G. Plaintiffs and Class Members Suffered Damages due to The Breach.

101. The Plaintiffs and Class Members have experienced considerable damage due to the exposure of their Private Information in the Data Breach.

102. The consequences of the Defendants' failure to secure the Class's Private Information are profound and enduring. Stolen Private Information can be fraudulently used for years, making victims of data breaches more susceptible to identity fraud.[14]

103. The Defendants' intentional, reckless, and negligent actions led to the Data Breach, allowing unauthorized access to, and misuse of, the Plaintiffs' and Class members' Private Information, placing them at an increased risk of identity theft and fraud.

104. The risks of identity theft are substantial, with victims facing extensive financial and reputational damage. Some may lose job opportunities or be denied loans due to affected credit records. In extreme cases, victims may even face wrongful arrest.

105. The Class faces ongoing risks of substantial fraud losses, including fraudulent online account charges, unauthorized loan applications, and various forms of identity theft. Many may already be unknowing victims of such crimes.

106. Plaintiffs and Class members have incurred, or will incur, expenses for protective measures like credit monitoring and credit freeze fees, directly related to the Data Breach.

107. The Plaintiffs and Class members did not receive the benefit of the bargain with their exchange with the Defendants, expecting robust data security in return for their private data,

[14] 2014 *LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

a standard the Defendants failed to meet. At the very least, the damages to the Plaintiffs and Class members are measurable as the difference in value between services expected (with adequate data security) and those actually received.

108. Plaintiffs and Class members would not have engaged with the Defendants had they known of the inadequate training, lack of safety controls, and poor data security practices. The Class will have to continue to invest significant time monitoring their financial accounts for misuse.

109. As a result of the Data Breach, Plaintiffs and Class members' Private Information has diminished in value.

110. The stolen Private Information can be used for various frauds, increasing the continuous risk of identity theft and related complications. Despite knowing these risks, the Defendants failed to adequately secure their data systems, leaving them vulnerable to a foreseeable data breach.

111. The Plaintiffs and Class Members' Private Information, which was inadequately protected by the Defendants, remained private and confidential until the Data Breach. The Defendants failed to obtain necessary consent for the disclosure of this information as mandated by relevant laws and industry standards, leading to an unauthorized release of their information due to poor security measures.

112. The Data Breach occurred as a direct consequence of the Defendants' failure to adequately secure and protect the Plaintiffs' and Class Members' Private Information from unauthorized access and use, violating state and federal regulations, industry norms, and common law. The Defendants also neglected to establish and maintain necessary safeguards to ensure the security and confidentiality of this information, leaving it vulnerable to foreseeable threats.

113. Despite having the means to prevent such a breach, the Defendants did not implement sufficient data security measures, neglecting their duty to protect customer data.

114. The Defendants' failure extends to inadequate training of employees, particularly within its IT department, to timely recognize and address cyber-attacks and other data security risks.

115. Proper rectification of its data security system flaws and adoption of expert-recommended security measures would have enabled the Defendants to prevent these system intrusions and the resulting theft of sensitive information.

116. Due to the Defendants' wrongful actions and omissions, the Plaintiffs and Class Members now face an imminent and ongoing risk of identity theft and fraud, compelling them to divert significant time and effort, which would otherwise be spent on personal and professional commitments, to mitigate the effects of the Data Breach.

117. The U.S. Department of Justice reports that resolving identity theft issues can be a lengthy process, with twenty-nine percent of victims spending over a month, with some taking a year just to address the fallout.[15]

118. Aside from offering a limited 12-month credit monitoring service, the Defendant has not taken any substantial steps to aid the Plaintiffs and Class Members in dealing with The Breach's aftermath.

119. This credit monitoring offer is grossly inadequate, as it does not preempt identity theft but merely alerts victims post-facto.[16] The gap between the acquisition and use of stolen information can be significant, leaving victims vulnerable for extended periods.

---

[15] *See* U.S. Dep't of Justice, Victims of Identity Theft, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf

[16] *See*, e.g., Kayleigh Kulp, Credit Monitoring Services May Not Be Worth the Cost, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

120. The Defendants' failure to protect Private Information has burdened the Plaintiffs and Class Members with significant time and financial costs to address and prevent potential fraud and identity theft, with the Defendant offering no assistance in these endeavors.

121. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have sustained and will continue to sustain economic loss and other harms. They have experienced and/or face an increased risk of experiencing the following forms of injuries:

a. Direct and indirect negative impacts on health and welfare, leading to permanent and irreversible consequences in their personal and professional lives:

i. theft of their PII;

ii. publication of their PII to the Dark Web;

iii. damages to and diminution in value of their PII;

iv. loss of the opportunity to control how their PII is used;

v. time spent on efforts to research how to prevent, detect, contest, and recover from misuse of PII;

vi. Emotional distress from the unauthorized disclosure of information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

vii. Continued risk of exposure to hackers and thieves of their information, which remains in Defendants' possession and is subject to further breaches so long as FNF fails to undertake appropriate and adequate measures to protect Plaintiffs' personal data.

b. Costs associated and time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of The Breach, including:

   i. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of PII, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards; imposing withdrawal and purchase limits on compromised accounts and other accounts subject to potential compromise; enrolling in credit monitoring and identity theft protection services;

   ii. money and time lost as a result of fraudulent access to and use of their financial accounts, and fraudulent charges, loss of use of and access to their financial accounts and/or credit, including loss of use and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

   iii. money and time expended to periodically order credit reports and place temporary freezes on credit, and to

   iv. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

   v. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

vi. anticipated future costs from the purchase of credit monitoring and identity theft protection services once the temporary services being offered by Defendants expire;

c. Costs associated with additional computer security needed due to increased personal vulnerability to cyber threats, including the enhanced risk of potential phishing attacks specifically crafted based on the extensive PII revealed, such as increased costs for anti-malware software and network security software and monitoring services on electronic devices, as well as increased time and effort to monitor for potential intrusions and respond to cyber security incidents on their personal devices and networks.

122. The stolen Private Information can be misused alone or combined with other data to facilitate further identity theft. Thieves might use this information for spear-phishing attacks, deceiving Class Members into revealing sensitive details.

123. Beyond tangible costs, there are also the intangible impacts such as the stress and anxiety associated with the constant threat of identity theft, and the potential emotional distress that arises from dealing with the consequences of a breach. Long-term effects of identity theft can include damage to credit scores, which in turn can affect the ability to obtain loans, housing, or even employment, leading to a loss of opportunities and potential income.

CLASS ACTION ALLEGATIONS

124. Plaintiffs bring all counts, as set forth below, individually and as a class action, pursuant to the provisions of Federal Rule of Civil Procedure 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class" (collectively, the "Class") defined as:

> All individuals who provided their Private Information to Dollar Tree and Zerod-In and whose Private Information was subsequently compromised as a result of the

> data breaches identified around August 2023. This class encompasses any person across the United States who falls within this criterion, regardless of their state of residence, encompassing a broad spectrum of individuals affected by The Breach of data security.

125. This class seeks to represent a collective group at the national level, uniting all affected individuals under a single legal action to address the common issue of the data breach and its consequences.

126. Excluded from the Nationwide Class are the Defendants themselves, along with their affiliates, parent companies, subsidiaries, officers, agents, and directors. This exclusion is to prevent any conflict of interest and ensure impartiality in the legal proceedings.

127. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

128. Numerosity (Rule 23(a)(1)): The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believes that the proposed Class includes hundreds of thousands of individuals who have been damaged by Defendants' conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendants' records.

129. Commonality and Predominance (Rules 23(a)(2) and 23(b)(3)): The Class shares common legal and factual questions, which are central to each member's case and outweigh any individual questions. These common issues include:

a. Compliance of Defendants' data security systems with data security laws and regulations, such as the FTCA;

b. Adherence of Defendants' data security systems to industry standards;

c. Effectiveness of Defendants' security measures in protecting the Class's Private Information;

d. Adequacy of Defendants' response in assessing the Data Breach;

e. Unauthorized disclosure of Private Information by the Defendants;

f. Breach of implied contract by the Defendants;

g. Failure of the Defendants to prevent unauthorized access due to willful, reckless, or negligent conduct;

h. Negligence of the Defendants in securing the Class's Private Information;

i. Defendants' unjust enrichment;

j. Entitlement of the Plaintiffs and the Class Members to damages and/or equitable relief.

130. The Defendants' actions have uniformly affected all Class members, resulting in similar violations, practices, and injuries. Any individual differences are minor compared to the predominant common questions in this case.

131. Typicality (Rule 23(a)(3)): The Plaintiffs' claims are typical of those of the Class, as all members have suffered similar harm due to the Defendants' uniform misconduct leading to the Data Breach. No unique defenses are applicable only to these Plaintiffs.

132. Adequacy of Representation (Rule 23(a)(4)): The Plaintiffs are suitable representatives of the Class, with aligned interests and no conflicts. They are represented by competent and experienced counsel and are committed to vigorously prosecuting the action, ensuring the Class's interests are adequately protected.

133. Injunctive Relief (Rule 23(b)(2)): The Defendants' actions, or inactions, affect the entire Class, warranting injunctive or declaratory relief.

134. Superiority (Rule 23(b)(3)): A class action is the most effective and efficient method for resolving this controversy. Individual litigation would be burdensome and

uneconomical due to the relatively small individual damages compared to litigation costs. The class action avoids inconsistent judgments and provides economies of scale, making it a preferable approach for both parties and the judicial system. Applicable to the whole Class.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of the Nationwide Class)

135. Plaintiffs and Class Members fully incorporate by reference all the above paragraphs, as though fully set forth herein.

136. This claim is brought by Plaintiffs individually and on behalf of the Class Members against Defendants Zeroed-In and Dollar Tree, Inc.

137. Defendants, in handling Plaintiffs' PII, owed Plaintiffs a duty to exercise reasonable care in safeguarding, securing, and protecting PII from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

138. This duty includes using reasonable care to prevent disclosure of Plaintiffs' PII and to ensure that it was adequately secured and protected by implementing processes by which it could promptly discover a breach of its security systems and prevent improper access and misuse of PII.

139. Defendants also owed a duty to Plaintiffs to give prompt notice to those who were affected in the case of a data breach that their information had been compromised in a timely manner, to the extent to which it was compromised, and the type of information that was compromised.

140. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and all Class Members' PII and the importance of maintaining secure systems.

Defendants knew or should have known of the many data breaches that have targeted companies that store PII in recent years and in light of the Defendants' deficient security protocols and practices.

141. Despite explicit commitments to adhere to industry standards and the duty of care owed, Defendants negligently and recklessly failed to implement, monitor, and maintain adequate data security measures and protocols.

142. The Defendants' breach of duty is starkly highlighted by the occurrence of the network breach. This breach serves as a clear indication of the Defendants' failure to uphold their responsibilities in several key aspects:

a. Inadequate Security Measures: The successful breach of the network suggests that the security measures in place were insufficient to protect against such intrusions. This inadequacy could stem from outdated security protocols, lack of robust firewalls, inadequate intrusion detection systems, or failure to implement industry-standard encryption methods.

b. Neglect in Regular System Updates and Maintenance: A breach often exploits vulnerabilities that could have been mitigated through regular system updates and maintenance. The Defendants' failure to ensure that their network systems were up to date with the latest security patches and defenses likely contributed to The Breach's success.

c. Lack of Vigilance and Monitoring: The occurrence of The Breach implies a potential lack of continuous monitoring and rapid response systems. Effective cybersecurity strategies require constant vigilance, including regular monitoring of network activities to detect and respond to suspicious behaviors promptly.

d. Ineffective Response Plans: The fact that The Breach occurred and was not immediately contained or mitigated points to a possible lack of effective incident response plans. Such plans are crucial for quickly addressing security breaches and minimizing their impact.

e. Failure to Adhere to Industry Standards and Best Practices: The Breach suggests a deviation from or inadequate adherence to established industry standards and best practices for data security. This includes not only technological measures but also policies, employee training, and regular security audits.

f. Overlooking Risks and Threat Assessments: The Defendants might not have adequately assessed the risks or understood the potential threats to their network, leading to a security posture that was ill-prepared to fend off The Breach.

g. Potential Complacency in Security Attitude: The Breach could indicate a level of complacency in the Defendants' approach to cybersecurity, possibly underestimating the sophistication or determination of cyber attackers.

143. Plaintiffs and Class Members had no ability to protect their information, so Defendants undertook the responsibility to safeguard Defendants' possession.

144. This failure resulted in a breach of their duty of care, leading to the compromise, unauthorized access, and potential misuse of Plaintiffs' sensitive PII.

145. The negligent conduct of Defendants directly caused foreseeable harm to Plaintiffs, including heightened risks of identity theft, unauthorized disclosure, and publication of PII, financial expenses incurred due to mitigating unauthorized use, and continued vulnerability of PII within Defendants' possession.

146. But for Defendants' wrongful and negligent breach of the duties owed to the Plaintiffs and Class Members, the Plaintiffs' PII would not have been compromised or misused.

147. Defendants' neglect in implementing adequate security measures directly links to the harm and imminent risk experienced by Plaintiffs and the Class Members. The loss and unauthorized access to their personal information occurred due to Defendants' failure to prudently safeguard this information through the adoption, implementation, and maintenance of suitable security measures.

148. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT II
NEGLIGENCE PER SE
Federal Trade Commission (FTC) ACT 15 U.S.C. § 45
(On Behalf of the Nationwide Class)

149. Plaintiffs and Class Members fully incorporate by reference all the above paragraphs, as though fully set forth herein.

150. This claim is brought by Plaintiffs individually and on behalf of the Class Members against Defendants Zeroed-In and Dollar Tree, Inc.

151. According to Section 5 of the FTC Act, which outlaws' unfair practices in commerce, entities like the Defendants are mandated to employ reasonable measures for the protection of personal information. This requirement is guided and enforced by the Federal Trade Commission (FTC), whose publications and directives outline the necessary data protection standards.

152. The FTC has determined that a company's neglect in upholding reasonable and appropriate data security measures for individuals' sensitive PII constitutes an "unfair practice,"

which is in direct contravention of the FTC Act 15 U.S.C. § 45. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

153. The Defendants had a duty of care towards the Plaintiffs and Class Members to ensure data security in line with industry standards and other related stipulations previously mentioned. This duty included maintaining their systems and networks, as well as the personnel managing them, to adequately safeguard the Plaintiffs' and Class Members' PII.

154. Defendants' duty of care to use reasonable security measures arose from the unique relationship established between Zeroed-In and the Plaintiffs and Class Members. This relationship was formed based on the trust placed in Zeroed-In by the Plaintiffs and Class Members who provided their confidential PII as part of their employment with Zeroed-In's clients, including Dollar Tree.

155. Defendants' duty to exercise due care in safeguarding confidential data was not only a result of the statutes and regulations described above but also due to industry norms mandating the protection of confidential PII.

156. The Defendants were subject to an "independent duty" to protect the Plaintiffs' and Class Members' data, a duty that existed irrespective of any contractual agreement between the Defendants and the Plaintiffs and Class Members.

157. The Defendants also had a duty to implement effective clearinghouse practices for the timely removal of PII belonging to former employees once its retention was no longer legally required. This duty was vital to ensure compliance with applicable data retention regulations.

158. Additionally, the Defendants had a duty to notify the Plaintiffs and Class Members promptly and effectively about the occurrence of the Data Breach, ensuring that those affected were fully informed.

159. Defendants had and continues to have duties to transparently disclose if the PII of the Plaintiffs and the Class Members within their possession was potentially compromised. This includes providing detailed information on the nature of the compromise, the specific types of data affected, and the exact timing of The Breach. This level of detailed notification is crucial in enabling those affected to understand the full scope and impact of The Breach.

160. Such comprehensive notification was essential to allow the Plaintiffs and the Class to take proactive measures to prevent, mitigate damages, and address any potential identity theft or fraudulent use of their PII by unauthorized third parties.

161. The Defendants breached these duties as outlined in the FTC Act and other relevant standards, demonstrating negligence by failing to implement reasonable security measures to protect the PII of the Class Members. Their specific negligent acts and omissions include, but are not limited to:

a. inadequately securing sensitive data,
b. failing to monitor their data systems effectively for potential breaches,
c. Failing to detect in a timely manner that Class Members' PII had been compromised,
d. not adhering to required data retention and disposal practices,
e. not providing timely or sufficient notification to those affected by the Data Breach.
f. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

162. The Defendants' inability to secure personal information adequately, alongside their failure to adhere to established industry standards, constitutes a blatant violation of Section 5 of the FTC Act. Their actions are particularly severe considering the substantial volume and

sensitive nature of the data they managed. Given this context, the Defendants could have reasonably anticipated the severe adverse consequences their conduct might have on the Plaintiffs and the Class.

163. It was foreseeable that the Defendants' negligence in implementing reasonable protective measures for the PII of Class Members could lead to significant harm. Moreover, the likelihood of a security breach was reasonably foreseeable, especially in light of the frequent incidents of cyberattacks and data breaches targeting companies that deal in PII.

164. Defendants have full knowledge of the sensitive nature of the PII they handled and understood the potential types of harm, including identity theft and privacy invasions, that the Plaintiffs and the Class would face if their PII were to be improperly disclosed.

165. Plaintiffs belong to the group of individuals that the FTC Act aims to protect, and the harm experienced by the compromise of their PII is precisely the type of harm the Act seeks to prevent.

166. As a direct and proximate result of the Defendants' negligence and negligence per se, the Plaintiffs have endured and will continue to face multiple forms of harm, including but not limited to:

a. Incidences of identity theft, with the associated risks and consequences;

b. Reduced control over how their personal information is used or shared;

c. Exposure, potential theft, and unauthorized use of their personal data;

d. Financial burdens related to the prevention, detection, and remediation of identity theft, tax fraud, or other misuses of personal information;

e. Lost time and productivity spent on addressing and mitigating the impacts of the Data Breach, including efforts to combat tax fraud and identity theft;

f. Costs incurred in placing credit freezes or fraud alerts on credit reports;

g. Continued vulnerability of their personal information, which remains at risk of further unauthorized access or misuse while under the Defendants' control;

h. Future anticipated costs in terms of time, effort, and finances to safeguard against ongoing risks.

167. The negligence per se of the Defendants has also led to significant non-economic damages for the Plaintiffs, manifesting as anxiety, emotional distress, and a loss of privacy, among other related adverse effects. These damages extend beyond tangible economic losses, significantly impacting the Plaintiffs' mental and emotional well-being.

168. The ongoing negligence and negligence per se of the Defendants have left the Plaintiffs and the Class Members in a state of continual vulnerability, with their personal information still under the Defendants' control and at risk of further breaches and unauthorized disclosures. This persistent exposure highlights the Defendants' continuous failure to implement and uphold necessary security and confidentiality measures for protecting such sensitive data.

169. But for Defendants' wrongful and negligent breaches of duties owed to Plaintiffs and the Class Members, the PII of Plaintiffs and the Class Members would not have been compromised.

170. There is a clear direct causal relationship between the Defendants' failure to establish adequate security measures and the subsequent harm, or the imminent risk of harm, that has befallen the Plaintiffs and Class Members. The unauthorized access and subsequent loss of the Plaintiffs' and Class Members' PII was a direct consequence of the Defendants' negligence in providing adequate security. This failure is characterized by a lack of proper adoption,

implementation, and maintenance of necessary and standard security measures crucial for the protection of sensitive PII.

171. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

173. Plaintiffs and Class Members fully incorporate by reference all the above paragraphs, as though fully set forth herein.

174. This claim is brought by Plaintiffs individually and on behalf of the Class Members against Defendants Zeroed-In and Dollar Tree, Inc.

175. An implied contract was established between the Defendants, Plaintiffs, and Class Members, based on the expectation that the Defendants would implement and maintain stringent data security measures to ensure the confidentiality of Plaintiffs' and Class Members' PII.

176. The Defendants required the provision of PII as a prerequisite for their services or employment, thereby compelling customers, Plaintiffs, and Class Members to trust them with their sensitive information.

177. The Defendants derived financial gains from the collection and use of the Plaintiffs and Class Members' personal information, which was a crucial aspect of their business operations. However, in this process, the Plaintiffs and Class Members did not receive the expected benefits from this exchange and were, instead, adversely affected.

178. The concept of "benefit of the bargain" implies that in a contractual agreement, all parties should receive the anticipated benefits as per the terms of the contract. Here, while the Defendants capitalized on the personal information for their financial and operational advantage, the Plaintiffs and Class Members did not receive the corresponding benefit, which would include the assurance of data security and privacy.

179. Plaintiffs and Class Members provided their PII to the Defendants under the presumption that it would be adequately protected and secured.

180. The Defendants routinely solicited the PII of Plaintiffs as part of their standard business transactions, which the Plaintiffs submitted in good faith.

181. The Defendants were obligated to diligently protect, secure, and safeguard the PII in their possession, including all information shared during business operations.

182. Given the history of data breaches in similar sectors, the Defendants should have been acutely aware of the risks involved in collecting and storing PII and the critical need for robust security measures.

183. The Defendants explicitly committed, via public statements and on their websites, to adhere to industry security standards and to ensure the protection of all PII under their control.

184. The Defendants breached these duties by failing to exercise the necessary care in the protection of Plaintiffs' PII, notably neglecting to implement and maintain adequate security measures.

185. Plaintiffs had no control or capability to protect their PII once it was in the possession of the Defendants.

186. It was reasonably foreseeable to the Defendants that neglecting proper security measures for PII would likely lead to unauthorized access or disclosure.

187. The unauthorized access and compromise of Plaintiffs' PII directly resulted from the Defendants' failure to establish and uphold adequate security measures, which was a breach of the implied contract.

188. The Defendants' actions and inactions led directly to the Data Breach, causing extensive harm to the Plaintiffs. This harm includes but is not limited to increased risks of identity theft, unauthorized use of compromised PII, financial burdens for preventive and corrective actions, ongoing risks associated with retained PII, future costs for continued vigilance and protection, overpayment for services rendered insecure, loss of privacy, and the diminished intrinsic value of their PII.

189. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

190. Plaintiffs and Class Members fully incorporate by reference all the above paragraphs, as though fully set forth herein.

191. This claim for unjust enrichment is presented alternatively to the previously mentioned Breach of Implied Contract claim (Count III).

192. This claim is brought by Plaintiffs individually and on behalf of the Class Members against Defendants Zeroed-In and Dollar Tree, Inc.

193. The Plaintiffs and Class Members conferred a tangible monetary benefit upon the Defendants. Specifically, they supplied employment services to Zeroed-In's clients, including Dollar Tree, during which they also provided their valuable PII to the Defendants. In return, they

were entitled to receive the agreed-upon services and the assurance of adequate data security for their PII.

194. The Defendants were fully aware of the benefits they received, namely the PII and associated services provided by the Plaintiffs and Class Members. They accepted and retained these benefits, leveraging the PII for their business advantage and profit.

195. However, the Defendants failed in their obligation to secure the PII, thereby not providing full compensation for the value that the Plaintiffs and Class Members' PII contributed.

196. The acquisition of the PII was marked by inequitable conduct, as the Defendants did not disclose their insufficient data security measures, as previously alleged.

197. Had the Plaintiffs and Class Members been aware of the Defendants' inadequate data security practices, they would not have entrusted their PII to the Defendants.

198. Presently, the Plaintiffs and Class Members lack an adequate legal remedy.

199. It is fundamentally unfair for the Defendants to retain the benefits conferred upon them under these circumstances, especially considering the harm suffered by the Plaintiffs and Class Members.

200. As a direct result of the Defendants' actions, the Plaintiffs and Class Members have endured various injuries, including but not limited to invasion of privacy, devaluation of their PII, lost time and opportunity costs in mitigating the Data Breach effects, loss of the expected value from their transactions, increased spam communications, and ongoing as well as elevated risk to their PII. This risk is compounded by the facts that their PII remains unencrypted and susceptible to further unauthorized access and is still retained by the Defendants without adequate protection measures.

201. The Plaintiffs and Class Members are entitled to full compensation from the Defendants, including refunds, restitution, or damages. Establishing a constructive trust from which they may seek restitution is a viable means of disgorging all profits, benefits, and compensation obtained by the Defendants through their wrongful actions.

202. Given the insufficiency of legal remedies, the Plaintiffs and Class Members assert this claim for unjust enrichment in conjunction or as an alternative to other claims presented in this case. This claim underscores the necessity of equitable relief to address the wrongs and losses incurred by the Plaintiff and Class Members due to the Defendants' actions.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. An order to certify the proposed Class, designating Plaintiffs and their legal counsel as representatives for the Class;

b. An award to the Plaintiffs and Class members of actual, statutory, punitive, and/or any other forms of damages as permissible under the cited statutes;

c. An order for the restitution, disgorgement, and/or other equitable remedies as allowed under the cited statutes or as deemed appropriate by the Court;

d. Orders mandating the Defendants to comprehensively address and rectify the impacts of the Data Breach;

e. Awards for pre-judgment and post-judgment interest to the Plaintiffs and Class members;

f. An award of treble damages, enhanced damages, and attorneys' fees as specified under the relevant statutes and associated laws;

g. An order granting reasonable attorneys' fees, costs of litigation, and expert witness fees to the Plaintiffs and the Class members;

h. Any additional relief that this Court finds just and appropriate in this situation.

JURY TRIAL IS DEMANDED

December 15, 2023

Respectfully Submitted,

PLAINTIFFS

By: */s/ Leonard A. Bennett*
Leonard A. Bennett, VSB #37523
Craig C. Marchiando, VSB #89736
John J. Maravalli, VSB #99000
Consumer Litigation Associates, P.C.
763 J. Clyde Morris Blvd., Suite 1-A
Newport News, VA 23601
Telephone: (757) 930-3660
Facsimile: (757) 930-3662
Email: lenbennett@clalegal.com
Email: craig@clalegal.com
Email: john@clalegal.com
Drew D. Sarrett, VSB #81658
Consumer Litigation Associates, P.C.
626 E. Broad Street, Suite 300
Richmond, VA 23219
Telephone: (804) 905-9900
Facsimile: (757) 930-3662
Email: drew@clalegal.com

Robert W. Murphy
Murphy Law Firm
440 Premier Circle
Suite 240
Charlottesville, Virginia 22901
Telephone: (434) 328-3100
Facsimile: (434) 328-3101
Email: rwmurphy@lawfirmmurphy.com